Amtsblatt
der Europäischen Union

DE
Reihe L

2024/1774

25.6.2024

DELEGIERTE VERORDNUNG (EU) 2024/1774 DER KOMMISSION

vom 13. März 2024

zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement und des vereinfachten IKT-Risikomanagementrahmens

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 [1], insbesondere auf Artikel 15 Unterabsatz 4 und Artikel 16 Absatz 3 Unterabsatz 4,

in Erwägung nachstehender Gründe:

(1) Die Verordnung (EU) 2022/2554 gilt für ein breites Spektrum von Finanzunternehmen, die sich in Bezug auf Größe, Struktur, interne Organisation sowie Art und Komplexität ihrer Tätigkeiten unterscheiden und daher mehr oder weniger Komplexitäts- oder Risikoelemente aufweisen. Um sicherzustellen, dass dieser Vielfalt gebührend Rechnung getragen wird, sollten sämtliche Anforderungen in Bezug auf Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit sowie einen vereinfachten IKT-Risikomanagementrahmen in einem angemessenen Verhältnis zu Größe, Struktur, interner Organisation, Art und Komplexität dieser Finanzunternehmen und den damit verbundenen Risiken stehen.

(2) Aus dem gleichen Grund sollten Finanzunternehmen, die der Verordnung (EU) 2022/2554 unterliegen, bei der Erfüllung der Anforderungen an Richtlinien, Verfahren, Protokolle und Tools für die IKT-Sicherheit sowie bei einem vereinfachten IKT-Risikomanagementrahmen über eine gewisse Flexibilität verfügen. Deshalb sollten Finanzunternehmen zur Erfüllung von Dokumentationsanforderungen, die sich aus diesen Anforderungen ergeben, sämtliche Unterlagen, über die sie bereits verfügen, verwenden dürfen. Die Entwicklung, Dokumentation und Umsetzung spezifischer Richtlinien für die IKT-Sicherheit sollte nur für bestimmte wesentliche Elemente verlangt werden, wobei auch die führenden Branchenpraktiken und -normen berücksichtigt werden sollten. Um spezifische technische Aspekte der Umsetzung abzudecken, müssen entsprechende Verfahren der IKT-Sicherheit entwickelt, dokumentiert und umgesetzt werden, unter anderem für das Kapazitäts- und Leistungsmanagement, den Umgang mit Schwachstellen und das Patch-Management, die Daten- und Systemsicherheit sowie die Protokollierung.

(3) Um die ordnungsgemäße Umsetzung der in Titel II Kapitel I genannten Richtlinien, Verfahren, Protokolle und Tools für die IKT-Sicherheit im Zeitverlauf zu gewährleisten, ist es wichtig, dass Finanzunternehmen alle Aufgaben und Zuständigkeiten im Zusammenhang mit der IKT-Sicherheit korrekt zuweisen und aufrechterhalten und dass sie festlegen, welche Folgen die Nichteinhaltung von Richtlinien oder Verfahren der IKT-Sicherheit hat.

(4) Um das Risiko von Interessenkonflikten zu begrenzen, sollten Finanzunternehmen bei der Zuweisung von IKT-Aufgaben und -Zuständigkeiten für Aufgabentrennung sorgen.

(5) Um Flexibilität zu gewährleisten und den Kontrollrahmen der Finanzunternehmen zu vereinfachen, sollten diese nicht verpflichtet sein, spezifische Bestimmungen über die Folgen der Nichteinhaltung der in Titel II Kapitel I genannten Richtlinien, Verfahren und Protokolle für die IKT-Sicherheit auszuarbeiten, wenn solche Bestimmungen bereits im Rahmen einer anderen solchen Richtlinie oder eines anderen solchen Verfahrens festgelegt sind.

[1] ABl. L 333 vom 27.12.2022, S. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(6) In einem dynamischen Umfeld, in dem ständig neue IKT-Risiken entstehen, ist es wichtig, dass Finanzunternehmen sich bei der Entwicklung von Richtlinien für die IKT-Sicherheit auf führende Verfahren und gegebenenfalls Normen im Sinne von Artikel 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates ([2]) stützen. Dies sollte es den in Titel II genannten Finanzunternehmen ermöglichen, in einer sich wandelnden Landschaft gut informiert und vorbereitet zu sein.

(7) Zur Gewährleistung der digitalen operationalen Resilienz sollten in Titel II genannte Finanzunternehmen im Rahmen ihrer Richtlinien, Verfahren, Protokolle und Tools für die IKT-Sicherheit eine Richtlinie für das Management von IKT-Assets, Verfahren für das Kapazitäts- und Leistungsmanagement sowie Richtlinien und Verfahren für IKT-Tätigkeiten entwickeln und umsetzen. Diese Richtlinien und Verfahren sind notwendig, um die Überwachung des Status von IKT-Assets während ihres gesamten Lebenszyklus zu gewährleisten, damit sie wirksam genutzt und gepflegt werden (Management von IKT-Assets). Diese Richtlinien und Verfahren sollten zudem eine Optimierung der IKT-Systeme gewährleisten und sicherstellen, dass die Leistung und die Kapazitäten der IKT-Systeme den für Betriebs- und Informationssicherheit formulierten Zielen gerecht werden (Kapazitäts- und Leistungsmanagement). Schließlich sollten diese Richtlinien und Verfahren gewährleisten, dass das laufende Management und der laufende Betrieb der IKT-Systeme (IKT-Tätigkeiten) wirksam und reibungslos vonstattengehen, und so das Risiko eines Verlusts der Vertraulichkeit, Integrität und Verfügbarkeit von Daten minimieren. Diese Richtlinien und Verfahren sind somit erforderlich, um die Sicherheit der Netzwerke zu gewährleisten, angemessene Schutzvorkehrungen gegen Eindringen und Datenmissbrauch zu bieten und die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten zu wahren.

(8) Um einen ordnungsgemäßen Umgang mit Risiken bei IKT-Altsystemem zu gewährleisten, sollten Finanzunternehmen Fristen für die Bereitstellung von IKT-Unterstützungsdiensten durch Dritte erfassen und überwachen. Angesichts der potenziellen Auswirkungen eines Verlusts der Vertraulichkeit, Integrität und Verfügbarkeit von Daten sollten sich Finanzunternehmen bei der Erfassung und Überwachung dieser Fristen auf IKT-Assets oder -Systeme konzentrieren, die für den Geschäftsbetrieb von kritischer Bedeutung sind.

(9) Kryptografische Kontrollen können die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten gewährleisten. In Titel II genannte Finanzunternehmen sollten daher solche Kontrollen auf der Grundlage eines risikobasierten Ansatzes festlegen und durchführen. Zu diesem Zweck sollten Finanzunternehmen in einem zweistufigen Prozess Daten einstufen und IKT-Risiken umfassend bewerten und im Anschluss daran betreffende Daten, die gespeichert sind oder übermittelt werden, und erforderlichenfalls auch solche, die gerade verwendet werden, entsprechend verschlüsseln. Angesichts der Komplexität der Verschlüsselung in Verwendung befindlicher Daten sollten die in Titel II dieser Verordnung genannten Finanzunternehmen solche Daten nur verschlüsseln, wenn dies angesichts der Ergebnisse der IKT-Risikobewertung angemessen ist. Wenn die Verschlüsselung in Verwendung befindlicher Daten nicht möglich oder zu komplex ist, sollten in Titel II genannte Finanzunternehmen in der Lage sein, die Vertraulichkeit, Integrität und Verfügbarkeit der betreffenden Daten durch andere Maßnahmen für IKT-Sicherheit zu schützen. Vor dem Hintergrund der raschen technologischen Entwicklung im Bereich der Kryptografie sollten in Titel II genannte Finanzunternehmen über Entwicklungen in der Kryptoanalyse auf dem Laufenden bleiben und führende Praktiken und Normen berücksichtigen. In Titel II genannte Finanzunternehmen sollten daher einen flexiblen Ansatz verfolgen, der auf Risikominderung und -überwachung beruht, sodass sie vor dem Hintergrund der Dynamik kryptografischer Bedrohungen in der Lage sind, solche Bedrohungen, einschließlich Bedrohungen aufgrund der Fortschritte im Bereich der Quantentechnologie, zu bewältigen.

(10) Die Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit und -Betrieb sind von wesentlicher Bedeutung für die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Ein zentraler Aspekt ist dabei die strikte Trennung der IKT-Produktionsumgebungen von Entwicklungs-, Test- und anderen Nicht-Produktionsumgebungen. Diese Trennung ist eine wichtige IKT-Sicherheitsmaßnahme gegen einen unbeabsichtigten und unbefugten Zugriff auf Daten und die Änderung und Löschung von Daten in der Produktionsumgebung, die zu größeren Störungen der Geschäftstätigkeit der in Titel II genannten Finanzunternehmen führen können. Gleichwohl sollte es Finanzunternehmen angesichts der derzeitigen IKT-Entwicklungsverfahren im Ausnahmefall gestattet sein, auch in Produktionsumgebungen zu testen, sofern sie diese Tests begründen und die erforderliche Genehmigung erhalten.

([2]) Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates (ABl. L 316 vom 14.11.2012, S. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(11) IKT-Landschaften, IKT-Schwachstellen und Cyberbedrohungen verändern sich ständig, sodass für die Ermittlung, Bewertung und Behebung von IKT-Schwachstellen ein proaktiver und umfassender Ansatz benötigt wird. Ohne einen solchen Ansatz drohen Finanzunternehmen, ihren Kunden, Nutzern und Gegenparteien erhebliche Risiken in Bezug auf ihre digitale operationale Resilienz, die Sicherheit ihrer Netzwerke und die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten, die durch Richtlinien und Verfahren der IKT-Sicherheit geschützt werden sollen. Daher sollten in Titel II genannte Finanzunternehmen Schwachstellen in ihrem IKT-Umfeld ermitteln und beheben, und sowohl Finanzunternehmen als auch ihre IKT-Drittdienstleister sollten in einem Rahmen arbeiten, der einen kohärenten, transparenten und verantwortungsvollen Umgang mit Schwachstellen gewährleistet. Aus demselben Grund sollten Finanzunternehmen IKT-Schwachstellen mithilfe zuverlässiger Ressourcen und automatisierter Tools überwachen und prüfen, ob IKT-Drittdienstleister bei Schwachstellen bereitgestellter IKT-Dienste unverzüglich aktiv werden.

(12) Patch-Management sollte ein wesentlicher Bestandteil dieser IKT-Sicherheitsrichtlinien und -verfahren sein, die dazu dienen, durch Erprobung und Einführung in einer kontrollierten Umgebung festgestellte Schwachstellen zu beseitigen und Störungen durch die Installation von Patches zu verhindern.

(13) Um im Hinblick auf potenzielle Sicherheitsbedrohungen, die für das Finanzunternehmen und seine Interessenträger relevant sein könnten, eine zeitnahe und transparente Kommunikation zu gewährleisten, sollten Finanzunternehmen Verfahren für eine verantwortungsvolle Offenlegung von IKT-Schwachstellen gegenüber Kunden, Gegenparteien und der Öffentlichkeit festlegen. Bei der Festlegung dieser Verfahren sollten Finanzunternehmen verschiedene Faktoren berücksichtigen und zum Beispiel prüfen, wie schwerwiegend die Schwachstelle ist, wie sie sich auf die Interessenträger auswirken kann und wie schnell für Abhilfe oder eine Minderung der Auswirkungen gesorgt werden kann.

(14) Bei der Zuweisung von Zugangsrechten an Nutzer sollten in Titel II genannte Finanzunternehmen durch strenge Maßnahmen sicherstellen, dass eine eindeutige Identifizierung von Personen und Systemen, die auf die Informationen des Finanzunternehmens zugreifen, gewährleistet ist. Wird dies versäumt, so setzt sich das betreffende Finanzunternehmen dem Risiko von potenziell unbefugten Zugriffen, Datenschutzverletzungen und betrügerischen Aktivitäten und somit der Gefahr einer Beeinträchtigung der Vertraulichkeit, Integrität und Verfügbarkeit sensibler Finanzdaten aus. Auch wenn die Verwendung von generischen oder gemeinsam genutzten Konten unter Umständen, die die Finanzunternehmen festlegen, ausnahmsweise zulässig sein sollte, sollten die Finanzunternehmen doch sicherstellen, dass Handlungen, die über diese Konten erfolgen, zurechenbar bleiben. Ist dies nicht der Fall, so bietet sich potenziellen böswilligen Nutzern die Möglichkeit, Ermittlungs- und Korrekturmaßnahmen zu behindern, was bei den Finanzunternehmen die Gefahr von unentdeckten böswilligen Handlungen oder von Sanktionen wegen Nichteinhaltung erhöhen würde.

(15) Angesichts der raschen Fortschritte in IKT-Umgebungen sollten die in Titel II genannten Finanzunternehmen robuste Richtlinien und Verfahren für das IKT-Projektmanagement implementieren, um die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten zu gewährleisten. In diesen Richtlinien und Verfahren für das IKT-Projektmanagement sollte festgelegt werden, welche Elemente für den Erfolg von IKT-Projekten erforderlich sind, einschließlich Änderungen, Beschaffung, Wartung und Entwicklung der IKT-Systeme des Finanzunternehmens, wobei es keine Rolle spielt, welche Methodik das Finanzunternehmen für das IKT-Projektmanagement gewählt hat. Im Rahmen dieser Richtlinien und Verfahren sollten Finanzunternehmen bedarfsgerechte Testverfahren und -methoden einführen, ohne jedoch Abstriche an ihrem risikobasierten Ansatz und einem sicheren, zuverlässigen und resilienten IKT-Umfeld zu machen. Zur Gewährleistung einer sicheren Durchführung von IKT-Projekten sollten Finanzunternehmen sicherstellen, dass Mitarbeiter aus bestimmten Geschäftsbereichen oder Funktionen, in denen das entsprechende IKT-Projekt Wirkung zeigen wird, die erforderlichen Informationen und Fachkenntnisse bereitstellen können. Um eine wirksame Aufsicht zu gewährleisten, sollten dem Leitungsorgan Berichte über IKT-Projekte und damit verbundene Risiken vorgelegt werden, insbesondere wenn diese Projekte kritische oder wichtige Funktionen betreffen. Finanzunternehmen sollten die Häufigkeit und die Einzelheiten der systematischen und laufenden Überprüfungen und Berichte auf Bedeutung und Umfang der betreffenden IKT-Projekte abstimmen.

(16) Softwarepakete, die in Titel II genannte Finanzunternehmen erwerben und entwickeln, müssen im Einklang mit den gesetzten Zielen für Betriebs- und Informationssicherheit wirksam und sicher in das bestehende IKT-Umfeld eingebunden werden. Finanzunternehmen sollten solche Softwarepakete daher gründlich bewerten. Zu diesem Zweck und zur Ermittlung von Schwachstellen und potenziellen Sicherheitslücken in den Softwarepaketen und den umfassenderen IKT-Systemen sollten Finanzunternehmen IKT-Sicherheitstests durchführen. Um die Integrität der Software zu bewerten und sicherzustellen, dass ihre Verwendung keine Risiken für die IKT-Sicherheit birgt, sollten Finanzunternehmen auch Quellcodes erworbener Software und nach Möglichkeit von IKT-Drittanbietern bereitgestellter proprietärer Software unter Verwendung statischer und dynamischer Testmethoden überprüfen.

(17) Änderungen bergen unabhängig von ihrem Umfang bestimmte inhärente Risiken, können erhebliche Risiken für den Verlust der Vertraulichkeit, Integrität und Verfügbarkeit von Daten mit sich bringen und somit zu schwerwiegenden Betriebsstörungen führen. Um Finanzunternehmen vor potenziellen IKT-Schwachstellen und damit verbundenen erheblichen Risiken zu schützen, wird ein strenges Überprüfungsverfahren benötigt, um festzustellen, ob Änderungen die erforderlichen IKT-Sicherheitsanforderungen erfüllen. Deshalb sollten sich die in Titel II genannten Finanzunternehmen solide Richtlinien und Verfahren für das IKT-Änderungsmanagement geben und diese als wesentliches Element ihrer Richtlinien und Verfahren für die IKT-Sicherheit behandeln. Um Objektivität und Wirksamkeit des IKT-Änderungsmanagements zu wahren, Interessenkonflikte zu vermeiden und eine objektive Bewertung von IKT-Änderungen sicherzustellen, müssen die für die Genehmigung dieser Änderungen zuständigen Funktionen von den Funktionen getrennt sein, die Änderungen anstoßen und umsetzen. Zur Gewährleistung eines wirksamen Übergangs, einer kontrollierten Umsetzung von IKT-Änderungen und minimaler Störungen des Betriebs der IKT-Systeme sollten Finanzunternehmen Rollen und Zuständigkeiten eindeutig zuweisen, um sicherzustellen, dass IKT-Änderungen gut geplant und angemessen getestet werden und dass Qualität gewährleistet ist. Ferner sollten Finanzunternehmen Ausweichverfahren entwickeln und umsetzen, die gewährleisten, dass IKT-Systeme weiterhin wirksam funktionieren, und für ein Sicherheitsnetz sorgen. Finanzunternehmen sollten diese Ausweichverfahren eindeutig definieren und die entsprechenden Zuständigkeiten zuweisen, um eine rasche und wirksame Reaktion auf nicht erfolgreich verlaufene IKT-Änderungen zu gewährleisten.

(18) Mit Blick auf die Erkennung, Steuerung und Meldung IKT-bezogener Vorfälle sollten in Titel II genannte Finanzunternehmen eine Strategie für IKT-bezogene Vorfälle mit den Komponenten eines IKT-Vorfallmanagements festlegen. Zu diesem Zweck sollten Finanzunternehmen alle relevanten Kontakte inner- und außerhalb der Organisation ermitteln, die eine ordnungsgemäße Koordinierung und Durchführung der verschiedenen Phasen dieses Prozesses unterstützen können. Zur Verbesserung der Erkennung IKT-bezogener Vorfälle und der Reaktion darauf und um bei diesen Vorfällen Trends zu ermitteln, die Finanzunternehmen wertvolle Informationen liefern können, um grundlegende Ursachen und Probleme wirksam auszumachen und anzugehen, sollten Finanzunternehmen IKT-bezogene Vorfälle und insbesondere solche, die sie unter anderem aufgrund ihres regelmäßigen Wiederauftretens für besonders wichtig halten, eingehend analysieren.

(19) Im Interesse einer frühzeitigen und wirksamen Aufdeckung von Anomalien sollten in Titel II genannte Finanzunternehmen unterschiedliche Informationsquellen erfassen, überwachen und analysieren und entsprechende Rollen und Zuständigkeiten zuweisen. Bei internen Informationsquellen sind Protokolle eine höchst relevante Quelle, doch sollten sich Finanzunternehmen nicht allein auf Protokolle verlassen. Stattdessen sollten sie umfassendere Informationen prüfen und auch Meldungen anderer interner Funktionen einbeziehen, die oft eine wertvolle Quelle relevanter Informationen sind. Aus dem gleichen Grund sollten Finanzunternehmen Informationen aus externen Quellen analysieren und überwachen, einschließlich der von IKT-Drittanbietern bereitgestellten Informationen über Vorfälle, die ihre Systeme und Netze betreffen, sowie anderer Informationsquellen, die Finanzunternehmen für relevant halten. Soweit personenbezogene Daten betroffen sind, findet das Datenschutzrecht der Union Anwendung. Die personenbezogenen Daten sollten auf das für die Erkennung des Vorfalls erforderliche Maß beschränkt sein.

(20) Zur Verbesserung der Erkennung IKT-bezogener Vorfälle sollten Finanzunternehmen diese Vorfälle dokumentieren. Um einerseits sicherzustellen, dass solche Nachweise ausreichend lang aufbewahrt werden, und andererseits einen übermäßigen Aufwand zu vermeiden, sollten Finanzunternehmen bei der Festlegung der Speicherfrist unter anderem die Kritikalität der betreffenden Daten und die sich aus dem Unionsrecht ergebenden Anforderungen an die Vorratsspeicherung berücksichtigen.

(21) Um sicherzustellen, dass IKT-bezogene Vorfälle zeitnah erkannt werden, sollten in Titel II genannte Finanzunternehmen sich nicht auf die Kriterien für die Erkennung IKT-bezogener Vorfälle und die Reaktion darauf beschränken. Finanzunternehmen sollten jedes dieser Kriterien berücksichtigen, doch sollten die Auslösung der Verfahren für die Erkennung IKT-bezogener Vorfälle und die Reaktion darauf nicht davon abhängen, dass die in den Kriterien beschriebenen Umstände gleichzeitig auftreten, und sollte die Bedeutung der betroffenen IKT-Dienste angemessen berücksichtigt werden.

(22) Bei der Entwicklung von IKT-Geschäftsfortführungsleitlinien sollten in Titel II genannte Finanzunternehmen die wesentlichen Komponenten des IKT-Risikomanagements berücksichtigen, darunter Management- und Kommunikationsstrategien für IKT-bezogene Vorfälle, Prozesse für das IKT-Änderungsmanagement und mit IKT-Drittanbietern verbundene Risiken.

(23) Es muss festgelegt werden, welche Szenarien in Titel II genannte Finanzunternehmen bei der Umsetzung ihrer IKT-Reaktions- und Wiederherstellungspläne und bei der Erprobung von IKT-Geschäftsfortführungsplänen berücksichtigen sollten. Diese Szenarien sollten den Finanzunternehmen als Ausgangspunkt für die Analyse von Relevanz und Plausibilität jedes Szenarios und der Notwendigkeit alternativer Szenarien dienen. Finanzunternehmen sollten sich auf Szenarien konzentrieren, in denen sich Investitionen in Resilienzmaßnahmen als besonders effizient und wirksam erweisen könnten. Durch Erprobung von Umstellungen von der primären IKT-Infrastruktur auf redundante Kapazitäten, Backups und redundante Systeme sollten die Finanzinstitute prüfen, ob diese Kapazitäten, Backups und Systeme während eines ausreichend langen Zeitraums wirksam funktionieren und sicherstellen, dass der normale Betrieb der primären IKT-Infrastruktur im Einklang mit den Wiederherstellungszielen wiederaufgenommen wird.

(24) Es werden Anforderungen bezüglich des operationellen Risikos benötigt, insbesondere Anforderungen an das IKT-Projekt- und Änderungsmanagement und die IKT-Geschäftsfortführung, die auf den Anforderungen aufbauen, die gemäß den Verordnungen (EU) Nr. 648/2012 ([3]), (EU) Nr. 600/2014 ([4]) und (EU) Nr. 909/2014 ([5]) des Europäischen Parlaments und des Rates bereits für zentrale Gegenparteien, Zentralverwahrer und Handelsplätze gelten.

(25) Gemäß Artikel 6 Absatz 5 der Verordnung (EU) 2022/2554 müssen Finanzunternehmen ihren IKT-Risikomanagementrahmen überprüfen und ihrer zuständigen Behörde einen Bericht über diese Überprüfung vorlegen. Damit die zuständigen Behörden die in diesen Berichten enthaltenen Informationen einfach verarbeiten können und eine angemessene Übermittlung dieser Informationen gewährleistet ist, sollten Finanzunternehmen diese Berichte in einem durchsuchbaren elektronischen Format übermitteln.

(26) Bei den Anforderungen an Finanzunternehmen, die dem in Artikel 16 der Verordnung (EU) 2022/2554 genannten vereinfachten IKT-Risikomanagementrahmen unterliegen, sollte der Schwerpunkt auf den wesentlichen Bereichen und Elementen liegen, die angesichts des Umfangs, des Risikos, der Größe und der Komplexität der betreffenden Finanzunternehmen mindestens erforderlich sind, um die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten und Dienste dieser Finanzunternehmen zu gewährleisten. Diese Finanzunternehmen sollten über einen internen Governance- und Kontrollrahmen mit klar festgelegten Zuständigkeiten verfügen, der die Grundlage für einen wirksamen und soliden Rahmen für das Risikomanagement bietet. Zur Verringerung des administrativen und operativen Aufwands sollten diese Finanzunternehmen nur eine Richtlinie entwickeln und dokumentieren, nämlich eine Richtlinie für Informationssicherheit, in der die übergeordneten Grundsätze und Vorschriften zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten und der Dienste dieser Finanzunternehmen festgelegt sind.

(27) Die Bestimmungen dieser Verordnung beziehen sich auf den IKT-Risikomanagementrahmen und legen spezifische Elemente, die gemäß Artikel 15 der Verordnung (EU) 2022/2554 für Finanzunternehmen gelten, sowie den vereinfachten IKT-Risikomanagementrahmen für die in Artikel 16 Absatz 1 der genannten Verordnung aufgeführten Finanzunternehmen fest. Um die Kohärenz zwischen dem normalen und dem vereinfachten IKT-Risikomanagementrahmen zu gewährleisten und um sicherzustellen, dass diese Bestimmungen zum gleichen Zeitpunkt anwendbar sind, ist es angezeigt, sie in einen einzigen Rechtsakt aufzunehmen.

(28) Diese Verordnung beruht auf dem Entwurf technischer Regulierungsstandards, der der Kommission von der Europäischen Bankenaufsichtsbehörde, der Europäischen Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung und der Europäischen Wertpapier- und Marktaufsichtsbehörde (Europäische Aufsichtsbehörden) in Absprache mit der Agentur der Europäischen Union für Cybersicherheit (ENISA) vorgelegt wurde.

([3]) Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister (ABl. L 201 vom 27.7.2012, S. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

([4]) Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 173 vom 12.6.2014, S. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

([5]) Verordnung (EU) Nr. 909/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 zur Verbesserung der Wertpapierlieferungen und -abrechnungen in der Europäischen Union und über Zentralverwahrer sowie zur Änderung der Richtlinien 98/26/EG und 2014/65/EU und der Verordnung (EU) Nr. 236/2012 (ABl. L 257 vom 28.8.2014, S. 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

(29) Der in Artikel 54 der Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates ([6]), in Artikel 54 der Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates ([7]) und in Artikel 54 der Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates ([8]) genannte Gemeinsame Ausschuss der Europäischen Aufsichtsbehörden hat zu diesem Entwurf technischer Regulierungsstandards, auf dem die vorliegende Verordnung beruht, öffentliche Konsultationen durchgeführt, die damit verbundenen Kosten- und Nutzeneffekte analysiert und die Stellungnahme der nach Artikel 37 der Verordnung (EU) Nr. 1093/2010 eingesetzten Interessengruppe Bankensektor, der nach Artikel 37 der Verordnung (EU) Nr. 1094/2010 eingesetzten Interessengruppe Versicherung und Rückversicherung und der nach Artikel 37 der Verordnung (EU) Nr. 1095/2010 eingesetzten Interessengruppe Wertpapiere und Wertpapiermärkte eingeholt.

(30) Soweit zur Erfüllung der in diesem Rechtsakt festgelegten Verpflichtungen die Verarbeitung personenbezogener Daten erforderlich ist, sollten die Verordnung (EU) 2016/679 ([9]) und die Verordnung (EU) 2018/1725 ([10]) des Europäischen Parlaments und des Rates uneingeschränkt Anwendung finden. Wenn beispielsweise personenbezogene Daten erhoben werden, um eine angemessene Erkennung von Vorfällen zu gewährleisten, sollte der Grundsatz der Datenminimierung eingehalten werden. Der Europäische Datenschutzbeauftragte wurde zum Entwurf dieses Rechtsakts konsultiert —

HAT FOLGENDE VERORDNUNG ERLASSEN:

TITEL I

ALLGEMEINER GRUNDSATZ

Artikel 1

Gesamtrisikoprofil und -komplexität

Bei der Entwicklung und Implementierung der Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit nach Titel II und des vereinfachten IKT-Risikomanagementrahmens nach Titel III werden Größe und Gesamtrisikoprofil des Finanzunternehmens sowie die Art und der Umfang seiner Dienstleistungen, Tätigkeiten und Geschäfte und die Elemente berücksichtigt, die deren Komplexität erhöhen oder verringern, darunter:

a) Verschlüsselung und Kryptografie;

b) IKT-Betriebssicherheit;

c) Netzwerksicherheit;

([6]) Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/79/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([9]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([10]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

d) IKT-Projekt- und -Änderungsmanagement;

e) die potenziellen Auswirkungen des IKT-Risikos auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten sowie von Störungen, die die Kontinuität und Verfügbarkeit der Tätigkeiten des Finanzunternehmens beeinträchtigen.

TITEL II

WEITERE HARMONISIERUNG VON TOOLS, METHODEN, PROZESSEN UND RICHTLINIEN FÜR IKT-RISIKOMANAGEMENT IM EINKLANG MIT ARTIKEL 15 DER VERORDNUNG (EU) 2022/2554

KAPITEL I

Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit

ABSCHNITT 1

Artikel 2

Allgemeine Elemente der Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit

(1) Die Finanzunternehmen stellen sicher, dass ihre IKT-Sicherheitsrichtlinien, die Informationssicherheit und die damit verbundenen Verfahren, Protokolle und Tools nach Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 in ihren IKT-Risikomanagementrahmen eingebettet sind. Die Finanzunternehmen legen Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit nach diesem Kapitel fest, die

a) die Netzwerksicherheit gewährleisten;

b) Schutzvorkehrungen gegen Eindringen und Missbrauch von Daten umfassen;

c) die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten wahren, einschließlich durch den Einsatz kryptografischer Techniken;

d) eine präzise und rasche Datenübermittlung ohne wesentliche Störungen und unangemessene Verzögerungen gewährleisten.

(2) Die Finanzunternehmen stellen sicher, dass die in Absatz 1 genannten IKT-Sicherheitsrichtlinien

a) auf die Ziele für die Informationssicherheit des Finanzunternehmens abgestimmt sind, die in der in Artikel 6 Absatz 8 der Verordnung (EU) 2022/2554 genannten Strategie für die digitale operationale Resilienz enthalten sind;

b) das Datum der förmlichen Genehmigung der IKT-Sicherheitsrichtlinien durch das Leitungsorgan enthalten;

c) Indikatoren und Maßnahmen für Folgendes umfassen:

   i) Überwachung der Implementierung der Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit,

   ii) Erfassung von Ausnahmen von dieser Implementierung,

   iii) Gewährleistung, dass bei Ausnahmen im Sinne von Ziffer ii die digitale operationale Resilienz des Finanzunternehmens sichergestellt ist;

d) die Verantwortlichkeiten der Mitarbeiter auf allen Ebenen festlegen, um die IKT-Sicherheit des Finanzunternehmens zu gewährleisten;

e) die Folgen einer Nichteinhaltung der IKT-Sicherheitsrichtlinien durch Mitarbeiter des Finanzunternehmens spezifizieren, sofern einschlägige Bestimmungen nicht in anderen Richtlinien des Finanzunternehmens enthalten sind;

f) ein Verzeichnis der erforderlichen Dokumentation umfassen;

g) die Regelungen für die Aufgabentrennung nach dem Modell der drei Verteidigungslinien oder gegebenenfalls einem anderen internen Modell für Risikomanagement und Kontrolle spezifizieren, um Interessenkonflikte zu vermeiden;

h) führende Praktiken und gegebenenfalls Normen im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 berücksichtigen;

i) die Aufgaben und Verantwortlichkeiten für die Entwicklung, Implementierung und Aufrechterhaltung von Richtlinien, Verfahren, Protokollen und Tools für IKT-Sicherheit festlegen;

j) im Einklang mit Artikel 6 Absatz 5 der Verordnung (EU) 2022/2554 überprüft werden;

k) wesentliche Änderungen in Bezug auf das Finanzunternehmen, einschließlich wesentlicher Änderungen der Tätigkeiten oder Prozesse des Finanzunternehmens, der Cyberbedrohungslage oder der geltenden rechtlichen Verpflichtungen, berücksichtigen.

ABSCHNITT 2

Artikel 3

IKT-Risikomanagement

Die Finanzunternehmen entwickeln, dokumentieren und implementieren Richtlinien und Verfahren für das IKT-Risikomanagement, die alle folgenden Elemente umfassen:

a) einen Verweis auf die Genehmigung der nach Artikel 6 Absatz 8 Buchstabe b der Verordnung (EU) 2022/2554 festgelegten Risikotoleranzschwelle für IKT-Risiken;

b) ein Verfahren und eine Methodik für die Durchführung der IKT-Risikobewertung, um Folgendes zu ermitteln:

   i) Schwachstellen und Bedrohungen, die die unterstützten Unternehmensfunktionen, die IKT-Systeme und die IKT-Assets, die diese Funktionen unterstützen, beeinträchtigen oder beeinträchtigen könnten,

   ii) die quantitativen oder qualitativen Indikatoren zur Messung der Auswirkungen und der Wahrscheinlichkeit eines Auftretens der unter Ziffer i genannten Schwachstellen und Bedrohungen;

c) das Verfahren zur Ermittlung, Implementierung und Dokumentation von Maßnahmen für die Behandlung von IKT-Risiken mit Blick auf die ermittelten und bewerteten IKT-Risiken, einschließlich der Festlegung von Maßnahmen für die Behandlung von IKT-Risiken, die erforderlich sind, um diese unter die Risikotoleranzschwelle nach Buchstabe a zu senken;

d) für IKT-Restrisiken, die nach der Implementierung der Maßnahmen für die Behandlung von IKT-Risiken gemäß Buchstabe c weiter bestehen:

   i) Bestimmungen über die Ermittlung dieser IKT-Restrisiken,

   ii) die Zuweisung von Aufgaben und Verantwortlichkeiten mit Blick auf

      1. das Eingehen von IKT-Restrisiken, die die Risikotoleranzschwelle nach Buchstabe a des Finanzunternehmens überschreiten,

      2. das Überprüfungsverfahren gemäß Buchstabe d Ziffer iv,

   iii) die Erstellung eines Inventars der eingegangenen IKT-Restrisiken, einschließlich einer Begründung, weshalb sie eingegangen wurden,

   iv) Bestimmungen über die Überprüfung der eingegangenen IKT-Restrisiken, die mindestens einmal jährlich vorgenommen wird, einschließlich zur

      1. Ermittlung etwaiger Änderungen der IKT-Restrisiken,

      2. Bewertung der verfügbaren Abhilfemaßnahmen,

      3. Bewertung, ob die Gründe für das Eingehen der IKT-Restrisiken zum Zeitpunkt der Überprüfung noch gültig und anwendbar sind;

e) Bestimmungen über die Überwachung

   i) jeglicher Änderungen der IKT-Risiken und der Cyberbedrohungslage,

   ii) interner und externer Schwachstellen und Bedrohungen,

   iii) des IKT-Risikos des Finanzunternehmens, damit Änderungen, die sich auf sein IKT-Risikoprofil auswirken könnten, rasch erkannt werden können;

f) Bestimmungen über ein Verfahren, mit dem sichergestellt wird, dass alle Änderungen der Geschäftsstrategie und der Strategie für die digitale operationale Resilienz des Finanzunternehmens berücksichtigt werden.

Für die Zwecke von Absatz 1 Buchstabe c stellt das dort genannte Verfahren sicher, dass

a) die Wirksamkeit der implementierten Maßnahmen für die Behandlung von IKT-Risiken überwacht wird;

b) bewertet wird, ob die festgelegten Risikotoleranzschwellen des Finanzunternehmens erreicht wurden;

c) bewertet wird, ob das Finanzunternehmen tätig geworden ist, um diese Maßnahmen erforderlichenfalls zu korrigieren oder zu verbessern.

ABSCHNITT 3

Management von IKT-Assets

Artikel 4

Richtlinie für das Management von IKT-Assets

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der in Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 genannten IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools eine Richtlinie für das Management von IKT-Assets.

(2) Die in Absatz 1 genannte Richtlinie für das Management von IKT-Assets enthält

a) Vorschriften für die Überwachung und das Management des Lebenszyklus von IKT-Assets, die gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 ermittelt und klassifiziert werden;

b) Vorschriften, wonach das Finanzunternehmen in seinen Aufzeichnungen Folgendes erfasst:

   i) die eindeutige Kennung jedes IKT-Assets,

   ii) Informationen über den physischen oder logischen Standort aller IKT-Assets,

   iii) die Klassifizierung aller IKT-Assets gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2022/2254,

   iv) die Identität der Eigentümer von IKT-Assets,

   v) die Unternehmensfunktionen oder -dienstleistungen, die durch das IKT-Asset unterstützt werden,

   vi) die für die IKT-Geschäftsfortführung geltenden Anforderungen, einschließlich der Vorgaben für die Wiederherstellungszeit und die Wiederherstellungspunkte,

   vii) die Möglichkeit eines Zugriffs auf das IKT-Asset über externe Netzwerke, einschließlich des Internets,

   viii) die Verbindungen und Interdependenzen zwischen IKT-Assets und den Unternehmensfunktionen, die die einzelnen IKT-Assets nutzen,

   ix) für alle IKT-Assets gegebenenfalls die Fristen bis zum Ende des Zeitraums, in dem die regelmäßigen, erweiterten und kundenspezifischen Unterstützungsdienstleistungen des IKT-Drittdienstleisters bereitgestellt werden und nach dem diese IKT-Assets nicht mehr von ihrem Anbieter oder einem IKT-Drittdienstleister unterstützt werden;

c) Vorschriften für Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, wonach diese Finanzunternehmen Aufzeichnungen über die Informationen führen, die für die Durchführung einer spezifischen IKT-Risikobewertung aller IKT-Altsysteme nach Artikel 8 Absatz 7 der Verordnung (EU) 2022/2554 erforderlich sind.

Artikel 5

Verfahren für das Management von IKT-Assets

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren ein Verfahren für das Management von IKT-Assets.

(2) In dem in Absatz 1 genannten Verfahren für das Management von IKT-Assets werden die Kriterien festgelegt, nach denen die Bewertung der Kritikalität von Informationsassets und IKT-Assets, die Unternehmensfunktionen unterstützen, vorgenommen wird. Bei dieser Bewertung wird Folgendes berücksichtigt:

a) das IKT-Risiko im Zusammenhang mit diesen Unternehmensfunktionen und deren Abhängigkeit von den Informationsassets oder IKT-Assets;

b) mögliche Auswirkungen des Verlusts der Vertraulichkeit, Integrität und Verfügbarkeit solcher Informationsassets und IKT-Assets auf die Geschäftsprozesse und -tätigkeiten der Finanzunternehmen.

ABSCHNITT 4

Verschlüsselung und Kryptografie

Artikel 6

Verschlüsselung und kryptografische Kontrollen

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der in Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 genannten IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools eine Richtlinie für Verschlüsselung und kryptografische Kontrollen.

(2) Die Finanzunternehmen konzipieren die in Absatz 1 genannte Richtlinie für Verschlüsselung und kryptografische Kontrollen auf der Grundlage der Ergebnisse einer genehmigten Datenklassifizierung sowie der IKT-Risikobewertung. Diese Richtlinie enthält Vorschriften zu allen folgenden Aspekten:

a) Verschlüsselung von Daten, die gespeichert sind oder gerade übermittelt werden;

b) Verschlüsselung von Daten, die gerade verwendet werden, soweit erforderlich;

c) Verschlüsselung der internen Netzwerkverbindungen und der Datenübermittlungen mit externen Parteien;

d) Management kryptografischer Schlüssel nach Artikel 7, um die Regeln für die korrekte Verwendung, den Schutz und den Lebenszyklus kryptografischer Schlüssel festzulegen.

Ist eine Verschlüsselung gerade verwendeter Daten nicht möglich, verarbeiten die Finanzunternehmen für die Zwecke von Buchstabe b gerade verwendete Daten in einer getrennten und geschützten Umgebung oder ergreifen gleichwertige Maßnahmen, um die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der Daten zu gewährleisten.

(3) Die Finanzunternehmen nehmen in die in Absatz 1 genannte Richtlinie für Verschlüsselung und kryptografische Kontrollen Kriterien für die Auswahl kryptografischer Techniken und Nutzungspraktiken auf, wobei führende Praktiken und Normen im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 sowie die Klassifizierung einschlägiger IKT-Assets gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 zu berücksichtigen sind. Finanzunternehmen, die nicht in der Lage sind, die führenden Praktiken oder Normen einzuhalten oder die zuverlässigsten Techniken anzuwenden, ergreifen Abhilfe- und Überwachungsmaßnahmen, die die Resilienz gegenüber Cyberbedrohungen gewährleisten.

(4) Die Finanzunternehmen nehmen in die in Absatz 1 genannte Richtlinie für Verschlüsselung und kryptografische Kontrollen Bestimmungen auf, in denen geregelt ist, wie die kryptografische Technologie aufgrund von Entwicklungen im Bereich der Kryptoanalyse gegebenenfalls zu aktualisieren oder zu ändern ist. Mit solchen Aktualisierungen oder Änderungen wird sichergestellt, dass die kryptografische Technologie nach Maßgabe von Artikel 10 Absatz 2 Buchstabe a gegen Cyberbedrohungen resilient bleibt. Finanzunternehmen, die nicht in der Lage sind, die kryptografische Technologie zu aktualisieren oder zu ändern, ergreifen Abhilfe- und Überwachungsmaßnahmen, die die Resilienz gegenüber Cyberbedrohungen sicherstellen.

(5) Die Finanzunternehmen nehmen in die in Absatz 1 genannte Richtlinie für Verschlüsselung und kryptografische Kontrollen eine Anforderung auf, nach der die Annahme von Abhilfe- und Überwachungsmaßnahmen im Einklang mit den Absätzen 3 und 4 aufzuzeichnen und zu begründen ist.

Artikel 7

Management kryptografischer Schlüssel

(1) Die Finanzunternehmen nehmen in die in Artikel 6 Absatz 2 Buchstabe d genannte Richtlinie für das Management kryptografischer Schlüssel Anforderungen auf, die für das Management kryptografischer Schlüssel über ihren gesamten Lebenszyklus hinweg gelten, einschließlich mit Blick auf die Generierung, Erneuerung, Speicherung, Sicherung, Archivierung, den Abruf, die Übermittlung, Rücknahme, den Widerruf und die Vernichtung dieser kryptografischen Schlüssel.

(2) Die Finanzunternehmen ermitteln und implementieren Kontrollen, um kryptografische Schlüssel während ihres gesamten Lebenszyklus vor Verlust, unbefugtem Zugriff, Offenlegung und Änderung zu schützen. Die Finanzunternehmen konzipieren diese Kontrollen auf der Grundlage der Ergebnisse der genehmigten Datenklassifizierung und der IKT-Risikobewertung.

(3) Die Finanzunternehmen entwickeln und implementieren Methoden, um die kryptografischen Schlüssel im Verlustfall oder bei Beeinträchtigungen oder Beschädigungen dieser Schlüssel auszutauschen.

(4) Die Finanzunternehmen erstellen und führen für mindestens diejenigen IKT-Assets, die kritische oder wichtige Funktionen unterstützen, ein Register aller Zertifikate und Zertifikatspeicher. Die Finanzunternehmen halten dieses Register auf dem neuesten Stand.

(5) Die Finanzunternehmen stellen sicher, dass die Zertifikate vor Ablauf unverzüglich erneuert werden.

ABSCHNITT 5

IKT-Betriebssicherheit

Artikel 8

Richtlinien und Verfahren für IKT-Vorgänge

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der in Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 genannten IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools Richtlinien und Verfahren für das Management der IKT-Vorgänge. In diesen Richtlinien und Verfahren wird festgelegt, wie Finanzunternehmen ihre IKT-Assets betreiben, überwachen, kontrollieren und wiederherstellen, einschließlich der Dokumentation der IKT-Vorgänge.

(2) Die in Absatz 1 genannten Richtlinien und Verfahren für IKT-Vorgänge enthalten alle folgenden Elemente:

a) eine Beschreibung der IKT-Assets, einschließlich aller folgenden Elemente:

   i) Anforderungen an die sichere Installation, Wartung, Konfiguration und Deinstallation eines IKT-Systems,

   ii) Anforderungen an das Management von Informationsassets, die von IKT-Assets genutzt werden, einschließlich ihrer automatisierten und manuellen Verarbeitung und Behandlung,

   iii) Anforderungen an die Ermittlung und Kontrolle von IKT-Altsystemen;

b) Kontrollen und Überwachung für IKT-Systeme, einschließlich aller folgenden Elemente:

   i) Anforderungen an die Sicherung und Wiederherstellung von IKT-Systemen,

   ii) Anforderungen an zeitliche Abläufe unter Berücksichtigung der Interdependenzen zwischen den IKT-Systemen,

   iii) Protokolle für Prüfpfad- und Systemprotokollinformationen,

   iv) Anforderungen, mit denen sichergestellt wird, dass bei der Durchführung einer internen Prüfung und anderer Tests Störungen des Geschäftsbetriebs minimiert werden,

   v) Anforderungen an die Trennung von IKT-Produktionsumgebungen von Entwicklungs-, Test- und anderen Nicht-Produktionsumgebungen,

   vi) Anforderungen hinsichtlich der Durchführung von Entwicklungs- und Testtätigkeiten in Umgebungen, die von der Produktionsumgebung getrennt sind,

   vii) Anforderungen im Zusammenhang mit Situationen, in denen die Entwicklungs- und Testtätigkeiten in Produktionsumgebungen durchgeführt werden;

c) Fehlerbehandlung bei IKT-Systemen, einschließlich aller folgenden Elemente:

i) Verfahren und Protokolle für die Fehlerbehandlung,

ii) Unterstützung und Ansprechpartner im Eskalationsfall, einschließlich externer Ansprechpartner für die Unterstützung im Falle unerwarteter operationaler oder technischer Probleme,

iii) Verfahren für den Neustart, das Zurücksetzen und die Wiederherstellung von IKT-Systemen im Falle einer Störung des IKT-Systems.

Für die Zwecke von Buchstabe b Ziffer v werden bei der Trennung alle Komponenten der Umgebung berücksichtigt, einschließlich Konten, Daten oder Verbindungen, wie in Artikel 13 Absatz 1 Buchstabe a festgelegt.

Für die Zwecke von Buchstabe b Ziffer vii ist in den in Absatz 1 genannten Richtlinien und Verfahren vorzusehen, dass die Fälle, in denen Tests in einer Produktionsumgebung durchgeführt werden, eindeutig zu identifizieren, zu begründen und zeitlich zu begrenzen sind und von der betreffenden Funktion im Einklang mit Artikel 16 Absatz 6 genehmigt werden. Die Finanzunternehmen stellen während der Entwicklungs- und Testtätigkeiten in der Produktionsumgebung die Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität von IKT-Systemen und -Produktionsdaten sicher.

Artikel 9

Kapazitäts- und Leistungsmanagement

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der in Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 genannten IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools Verfahren für das Kapazitäts- und Leistungsmanagement, die Folgendes betreffen:

a) die Ermittlung der Anforderungen an die Kapazität ihrer IKT-Systeme,

b) die Anwendung von Methoden zur Ressourcenoptimierung,

c) Überwachungsverfahren, um Folgendes aufrechtzuerhalten und zu verbessern:

i) die Verfügbarkeit von Daten und IKT-Systemen,

ii) die Effizienz der IKT-Systeme,

iii) die Verhinderung von IKT-Kapazitätsengpässen.

(2) Durch die in Absatz 1 genannten Verfahren für das Kapazitäts- und Leistungsmanagement wird sichergestellt, dass die Finanzunternehmen geeignete Maßnahmen ergreifen, um den Besonderheiten von IKT-Systemen mit langen oder komplexen Beschaffungs- oder Genehmigungsverfahren oder von ressourcenintensiven IKT-Systemen Rechnung zu tragen.

Artikel 10

Schwachstellen- und Patch-Management

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der in Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 genannten IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools Verfahren für das Schwachstellen-Management.

(2) Die in Absatz 1 genannten Verfahren für das Schwachstellen-Management sorgen dafür, dass

a) relevante und vertrauenswürdige Informationsressourcen ermittelt und aktualisiert werden, um für Schwachstellen zu sensibilisieren und das Bewusstsein dafür aufrechtzuerhalten,

b) die Durchführung automatisierter Schwachstellenbewertungen und -scans bei IKT-Assets gewährleistet und dabei sichergestellt wird, dass deren Häufigkeit und Umfang der im Einklang mit Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 festgelegten Klassifizierung und dem Gesamtrisikoprofil des IKT-Assets entsprechen,

c) überprüft wird, ob

i) IKT-Drittdienstleister Schwachstellen angehen, die im Zusammenhang mit den IKT-Dienstleistungen für das Finanzunternehmen stehen,

ii) diese Dienstleister dem Finanzunternehmen zumindest die kritischen Schwachstellen und Statistiken und Trends zeitnah melden;

d) nachverfolgt wird, wie Folgendes verwendet wird:

i) Bibliotheken Dritter, einschließlich Open-Source-Bibliotheken, die für IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen genutzt werden,

ii) IKT-Dienstleistungen, die das Finanzunternehmen selbst entwickelt hat oder von einem IKT-Drittdienstleister speziell für das Finanzunternehmen angepasst oder entwickelt wurden;

e) Verfahren für die verantwortungsvolle Offenlegung von Schwachstellen gegenüber Kunden, Gegenparteien und der Öffentlichkeit festgelegt werden,

f) die Einführung von Patches und anderen Abhilfemaßnahmen priorisiert wird, um die ermittelten Schwachstellen zu beheben,

g) die Behebung von Schwachstellen überwacht und geprüft wird,

h) eine Aufzeichnung aller festgestellten Schwachstellen, die IKT-Systeme betreffen, und die Überwachung der Behebung dieser Schwachstellen verlangt werden.

Für die Zwecke von Buchstabe b führen die Finanzunternehmen die automatisierten Schwachstellenbewertungen und -scans für IKT-Assets bei IKT-Assets, die kritische oder wichtige Funktionen unterstützen, mindestens einmal wöchentlich durch.

Für die Zwecke von Buchstabe c fordern die Finanzunternehmen IKT-Drittdienstleister auf, die einschlägigen Schwachstellen zu untersuchen, die Ursachen zu ermitteln und geeignete Abhilfemaßnahmen zu ergreifen.

Für die Zwecke von Buchstabe d überwachen die Finanzunternehmen, gegebenenfalls in Zusammenarbeit mit dem IKT-Drittdienstleister, die aktuelle Version der Bibliotheken Dritter sowie mögliche Aktualisierungen. Was gebrauchsfertige (Standard-)IKT-Assets oder Komponenten von IKT-Assets betrifft, die für die Ausführung von IKT-Dienstleistungen erworben und verwendet werden, die keine kritischen oder wichtigen Funktionen unterstützen, wird die Nutzung von Bibliotheken Dritter, einschließlich Open-Source-Bibliotheken, von den Finanzunternehmen soweit wie möglich nachverfolgt.

Für die Zwecke von Buchstabe f berücksichtigen die Finanzunternehmen die Kritikalität der Schwachstelle, die im Einklang mit Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 festgelegte Klassifizierung sowie das Risikoprofil der IKT-Assets, die von den ermittelten Schwachstellen betroffen sind.

(3) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der in Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 genannten IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools Verfahren für das Patch-Management.

(4) Die in Absatz 3 genannten Verfahren für das Patch-Management dienen dazu,

a) soweit möglich verfügbare Software- und Hardware-Patches und -Aktualisierungen mithilfe automatisierter Tools zu ermitteln und zu bewerten;

b) Notfallverfahren für das Patching und die Aktualisierung von IKT-Assets zu ermitteln;

c) Software- und Hardware-Patches und die Aktualisierungen gemäß Artikel 8 Absatz 2 Buchstabe b Ziffern v, vi und vii zu testen und einzuführen;

d) Fristen für die Installation von Software- und Hardware-Patches und von Aktualisierungen zu setzen sowie Eskalationsverfahren für den Fall festzulegen, dass diese Fristen nicht eingehalten werden können.

Artikel 11

Daten- und Systemsicherheit

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der in Artikel 9 Absatz 2 der Verordnung (EU) 2022/2554 genannten IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools ein Verfahren für die Daten- und Systemsicherheit.

(2) Das in Absatz 1 genannte Verfahren für die Daten- und Systemsicherheit umfasst alle folgenden Elemente im Zusammenhang mit der Daten- und IKT-Systemsicherheit im Einklang mit der gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 festgelegten Klassifizierung:

a) die in Artikel 21 dieser Verordnung genannten Zugangsbeschränkungen zur Unterstützung der Anforderungen im Zusammenhang mit dem Schutz für jede Klassifizierungsstufe;

b) die Ermittlung von Mindestanforderungen an eine sichere Konfigurationsbasis für IKT-Assets, durch die die Exposition dieser IKT-Assets gegenüber Cyberbedrohungen minimiert wird, sowie Maßnahmen zur regelmäßigen Überprüfung, ob diese Mindestanforderungen wirksam verwendet werden;

c) die Ermittlung von Sicherheitsmaßnahmen, um zu gewährleisten, dass ausschließlich zugelassene Software in IKT-Systemen und Endgeräten installiert wird;

d) die Ermittlung von Sicherheitsmaßnahmen gegen Schadprogramme;

e) die Ermittlung von Sicherheitsmaßnahmen, um zu gewährleisten, dass ausschließlich zugelassene Datenträger, Systeme und Endgeräte für die Übermittlung und Speicherung von Daten des Finanzunternehmens verwendet werden;

f) die folgenden Anforderungen, um die sichere Nutzung tragbarer Endgeräte und privater nicht tragbarer Endgeräte zu gewährleisten:

   i) die Anforderung einer Lösung für das Management der Endgeräte und die Löschung von Daten des Finanzunternehmens durch Fernzugriff,

   ii) die Anforderung, Sicherheitsmechanismen zu verwenden, die von den Mitarbeitern oder IKT-Drittdienstleistern nicht auf unbefugte Weise geändert, entfernt oder umgangen werden können,

   iii) die Anforderung, mobile Datenspeicher nur dann zu verwenden, wenn das IKT-Restrisiko unter der in Artikel 3 Absatz 1 Buchstabe a genannten Risikotoleranzschwelle des Finanzunternehmens liegt;

g) das Verfahren zur sicheren Löschung von Daten in den Räumlichkeiten des Finanzunternehmens oder von extern gespeicherten Daten, die das Finanzunternehmen nicht mehr erheben oder speichern muss;

h) das Verfahren zur sicheren Entsorgung oder Außerbetriebnahme von Datenspeichern in den Räumlichkeiten des Finanzunternehmens oder von extern aufbewahrten Datenspeichern, die vertrauliche Informationen enthalten;

i) die Ermittlung und Implementierung von Sicherheitsmaßnahmen zur Verhinderung von Datenverlust und Datenlecks bei Systemen und Endgeräten;

j) die Implementierung von Sicherheitsmaßnahmen, um zu gewährleisten, dass Telearbeit und die Nutzung privater Endgeräte nicht die IKT-Sicherheit des Finanzunternehmens beeinträchtigen;

k) für IKT-Assets oder -Dienstleistungen, die von einem IKT- Drittdienstleister betrieben werden, die Ermittlung und Umsetzung von Anforderungen an die Aufrechterhaltung der digitalen operationalen Resilienz im Einklang mit den Ergebnissen der Datenklassifizierung und der IKT-Risikobewertung.

Für die Zwecke von Buchstabe b werden im Rahmen der dort genannten sicheren Konfigurationsbasis die führenden Praktiken und geeigneten Techniken berücksichtigt, die in den Normen im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 festgelegt sind.

Für die Zwecke von Buchstabe k berücksichtigen Finanzunternehmen Folgendes:

a) die Implementierung der vom Anbieter empfohlenen Einstellungen für Komponenten, die vom Finanzunternehmen betrieben werden;

b) eine klare Aufteilung der die Informationssicherheit betreffenden Aufgaben und Verantwortlichkeiten zwischen dem Finanzunternehmen und dem IKT-Drittdienstleister im Einklang mit dem in Artikel 28 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannten Grundsatz der vollen Verantwortlichkeit des Finanzunternehmens für seinen IKT-Drittdienstleister und für Finanzunternehmen nach Artikel 28 Absatz 2 der genannten Verordnung sowie im Einklang mit der Richtlinie des Finanzunternehmens für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen;

c) die Notwendigkeit, innerhalb des Finanzunternehmens angemessene Kompetenzen für das Management und die Sicherheit der in Anspruch genommenen Dienstleistungen sicherzustellen und aufrechtzuerhalten;

d) technische und organisatorische Maßnahmen zur Minimierung der Risiken im Zusammenhang mit der Infrastruktur, die der IKT-Drittdienstleister für seine IKT-Dienstleistungen nutzt, unter Berücksichtigung führender Praktiken und Normen im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012.

Artikel 12

Datenaufzeichnung

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der Schutzvorkehrungen gegen Eindringen und Missbrauch von Daten Verfahren, Protokolle und Tools für die Datenaufzeichnung.

(2) Die in Absatz 1 genannten Verfahren, Protokolle und Tools für die Datenaufzeichnung umfassen alle folgenden Elemente:

a) die Ermittlung der aufzuzeichnenden Ereignisse, die Speicherfrist für die Datenaufzeichnungen und die Maßnahmen zur Sicherung und Verarbeitung der Aufzeichnungsdaten unter Berücksichtigung des Zwecks, für den die Datenaufzeichnungen erstellt werden;

b) die Abstimmung des Detaillierungsgrads der Datenaufzeichnungen auf deren Zweck und Verwendung, um die wirksame Erkennung anomaler Aktivitäten nach Artikel 24 zu ermöglichen;

c) die Anforderung, Ereignisse aufzuzeichnen, die sämtliche der folgenden Aspekte betreffen:

   i) logische und physische Zugangskontrolle nach Artikel 21 und Identitätsmanagement,

   ii) Kapazitätsmanagement,

   iii) Änderungsmanagement,

   iv) IKT-Vorgänge, einschließlich IKT-Systemaktivitäten,

   v) Netzwerkverkehrsaktivitäten, einschließlich der Leistung der IKT-Netzwerke;

d) Maßnahmen zum Schutz von Datenaufzeichnungssystemen und -informationen vor Manipulation, Löschung und unbefugtem Zugriff mit Blick auf gespeicherte, übermittelte oder gegebenenfalls gerade verwendete Daten;

e) Maßnahmen zur Erkennung eines Ausfalls von Datenaufzeichnungssystemen;

f) unbeschadet etwaiger im Unionsrecht oder nationalen Recht festgelegter anwendbarer rechtlicher Anforderungen die Synchronisierung der Uhren jedes IKT-Systems des Finanzunternehmens auf der Grundlage einer dokumentierten zuverlässigen Referenzzeitquelle.

Für die Zwecke von Buchstabe a legen die Finanzunternehmen die Speicherfrist fest und tragen dabei den Geschäftszielen und den Zielen für die Informationssicherheit, dem Grund, weshalb das Ereignis aufgezeichnet wurde, und den Ergebnissen der IKT-Risikobewertung Rechnung.

Abschnitt 6

Netzwerksicherheit

Artikel 13

Management der Netzwerksicherheit

Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der Schutzvorkehrungen, die die Sicherheit der Netzwerke gegen Eindringen und Missbrauch von Daten gewährleisten, Richtlinien, Verfahren, Protokolle und Tools für das Management der Netzwerksicherheit, in denen alle folgenden Aspekte behandelt werden:

a) die Trennung und Segmentierung von IKT-Systemen und -Netzwerken unter Berücksichtigung

   i) der Kritikalität oder Bedeutung der Funktion, die von diesen IKT-Systemen und -Netzwerken unterstützt wird,

   ii) der im Einklang mit Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 festgelegten Klassifizierung,

   iii) des Gesamtrisikoprofils der IKT-Assets, die diese IKT-Systeme und -Netzwerke nutzen;

b) die Dokumentation aller Netzwerkverbindungen und Datenflüsse des Finanzunternehmens;

c) die Nutzung eines gesonderten und speziellen Netzwerks für die Verwaltung von IKT-Assets;

d) die Ermittlung und Implementierung von Kontrollen für den Netzwerkzugang, um Verbindungen zum Netzwerk des Finanzunternehmens durch ein nicht zugelassenes Gerät oder System oder einen Endpunkt, der die Sicherheitsanforderungen des Finanzunternehmens nicht erfüllt, zu verhindern und zu erkennen;